REMARKS

The Final Office Action mailed March 5, 2009 considered claims 1-20. Claims 1-20 were rejected under 35 U.S.C. 103(a) as being unpatentable over White et al. ("Anatomy of a Commercial-Grade Immune System") hereinafter *White* in view of Schultz et al. (US 2003/0065926) hereinafter *Schultz*.[1]

A. Rejection under 35 U.S.C. 103(a)

Applicant respectfully traverses the rejection of claims 1-20 under 35 U.S.C. 103(a) over *White* in view of *Schultz* at least because there is no teaching, suggestion, motivation or other reason for modifying or combining the cited references as proposed by the Office Action.

Nevertheless, to expedite allowance, Applicant amended claims 1 and 2 to recite, among other things, "a plurality of different execution behaviors of the code module are recorded into a behavior signature corresponding to the code module" and that "the malware detection system is configured to report whether the code module is a known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match a plurality of different execution behaviors recorded in a behavior signature of the known malware."

In addition, Applicant amended claim 3 to recite, among other things, "recording a plurality of different execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module during execution of the code module" and "reporting whether the code module is the known malware based at least in part on the degree that the plurality of different execution behaviors recorded in the behavior signature of the code module match the plurality of different execution behaviors of the behavior signature of the known malware."

Applicant also amended claim 4 to recite, among other things, "recording a plurality of different execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module as the code module is executing" and "reporting whether the code module is the known malware based at least in part on the degree that the plurality of different execution

[1] Although the prior art status of the cited art is not being challenged at this time, Applicant reserves the right to challenge the prior art status of the cited art at any appropriate time, should it arise. Accordingly, any arguments and amendments made herein should not be construed as acquiescing to any prior art status of the cited art.

behaviors recorded in the behavior signature of the code module match the plurality of different execution behaviors of the behavior signature of the known malware."

Thus, the independent claims 1-4 each recite, among other things, features relating to (1) executing a code module and recording a plurality of different behaviors that resulted and (2) comparing those different, actually executed behaviors with a plurality of different behaviors of a behavior signature of a particular known malware, which allows the system to report whether the code module is the particular known malware.

In contrast, neither *White* nor *Schultz* discloses comparing a code module's plurality of different, executed behaviors with a plurality of different behaviors of a behavior signature of a particular known malware. Moreover, neither *White* nor *Schultz* discloses reporting whether that code module is the particular known malware based on that comparison.

Schultz merely uses a pattern matching of code segments to identify whether a program is malicious in general.[2] *Schultz* doesn't execute the program to identify behavior and certainly doesn't report that the program is a particular known malware based on such behavior. In fact, *Schultz* teaches away from executing the program: "All of the information about the binary is obtained from the program without executing the unknown program by by examining the static properties of the binary…."[3]

White merely discloses a replication environment used to identify a single behavior: replication.[4] *White* doesn't use this fact (*i.e.*, the fact that a sample replicated itself) to determine that the sample is a particular virus. Instead, it merely determines that the sample is a virus and then generates a bit sequence signature string from the sample to be used to identify future viruses.[5] As discussed in background of the present application, hash sequences like this are inadequate because malware can be easily modified and thus the hash sequences of the modified malware do not match the hash sequences of the original, unmodified malware.

Accordingly, independent claims 1-4 are allowable over the cited references at least because the cited references, either alone or in combination, fail to include each recited feature in the claims. The remaining claims depend from one of these independent claims and therefore are allowable for at least the same reasons as the independent claims.

[2] *See Schultz*, ¶ [0043] (discussing a hexidecimal representation of the executable machine code).
[3] *See Schultz*, ¶ [0044] (emphasis added).
[4] *See* White, at 20-21.
[5] *See* White, at 21 (discussing extracting "a good signature string").

In view of the foregoing, Applicant respectfully submits that the other rejections to the claims are now moot and do not, therefore, need to be addressed individually at this time. It will be appreciated, however, that this should not be construed as Applicant acquiescing to any of the purported teachings or assertions made in the last action regarding the cited art or the pending application, including any official notice. Instead, Applicant reserves the right to challenge any of the purported teachings or assertions made in the last action at any appropriate time in the future, should the need arise. Furthermore, to the extent that the Examiner has relied on any Official Notice, explicitly or implicitly, Applicant specifically requests that the Examiner provide references supporting the teachings officially noticed, as well as the required motivation or suggestion to combine the relied upon notice with the other art of record.

In the event that the Examiner finds remaining impediment to a prompt allowance of this application that may be clarified through a telephone interview, the Examiner is requested to contact the undersigned attorney at (801) 533-9800.

Dated this 2nd day of July, 2009.

Respectfully submitted,

RICK D. NYDEGGER
Registration No. 28,651
MICHAEL B. DODD
Registration No. 46,437
Attorneys for Applicant
Customer No. 47973

RDN:MBD:crb
2387791_1.DOC